FSA Integration Partner

United States Department of Education

Federal Student Aid

Data Strategy Enterprise-Wide Enrollment and Access Management Team 123.1.27 Access Management Business Objectives and High Level Requirements

Task Order #123

Version 1.0

June 30, 2003

Executive Summary

The Enrollment and Access Management initiative reviews FSA's existing offerings for Enrollment and Access Management and documents FSA's Business Objectives and High-Level Requirements. This document is the first step in formulating a high-level design for implementing a new vision.

Currently, enrollment and access management processes and tools operate on a non-centralized, non-standardized basis. As a result, Trading Partner interactions with FSA systems are fragmented and complex. In addition, these processes have often been inconsistently implemented particularly relating to user access rights.

Application reviews were conducted for each FSA system. These reviews captured current Enrollment and Access Management procedures. As a result of these sessions, several observations were made. Most prominently, inconsistent implementations have created points of confusion among Trading Partners regarding enrollment and access management procedures.

Initial system meetings facilitated the first stage of gathering business objectives and high-level requirements. Further exploration of FSA's business needs occurred during Core Team and Business Objective Meetings. These sessions included representatives from the Delivery and Eligibility, Servicing, and Applications areas.

The participants reached consensus on the following stated objectives and requirements, which were analyzed and aggregated into 16 business objectives and 70 high-level requirements. Of the business objectives identified, five business objectives are Access Management specific:

- A2.3 - Balance easier access and system security.
- B1.1 - Adopt a uniform decision making process for evaluating users requesting access to FSA systems.
- B2.1 - Provide effective oversight of user access to FSA systems.
- C2.2 - Maintain security of FSA systems.
- C2.3 - Provide users with access to FSA systems appropriate for their job function.

The other 11 Business Objectives are both Enrollment and Access Management focused and are contained in the accompanying Enrollment Business Objectives and High-Level Requirements deliverable:

- A1.1 - Focus on registration processes and access decisions at the enterprise level instead of on a per system basis.
- A2.1 - Manage enrollment and access privileges at the enterprise level.
- A2.2 - Improve self-service capabilities.
- A2.4 - The enrollment and access solution should be flexible enough to support the requirements of current and future FSA systems.

- A2.5 - Allow users to customize their experience with FSA systems.
- A3.1 - Streamline enrollment and access management for Trading Partner services.
- B3.1 - Meet FSA regulatory compliance requirements.
- C1.1 - Facilitate access to sets of data at the enterprise level.
- C2.1 - Create enterprise policy and standards for enrollment and access management.
- C3.1 - Provide effective training and customer support across FSA systems.
- C3.2 - Adopt enrollment and access management policies that improve business processes.

The process of analyzing the current environment and documenting business objectives produced the following guiding principles that will drive the High-Level Design:

- **Balance of Access and Security** - FSA wishes to create more efficient and easier-to-use processes, but not at the expense of controls to protect FSA resources.
- **Solution Flexibility** - FSA systems will not remain static. Enrollment and access management solutions need to be flexible and accommodate the requirements of future system reengineering and consolidation efforts.
- **Technology** - Many of the FSA high-level requirements involve new functions that may require technical solutions. Examples identified include single sign-on functions, automation of enrollment and access management, and user self-service capabilities. Before technology is incorporated into the FSA vision or high-level designs, FSA must balance cost and functionality.
- **Effective Communication Processes** - Enrollment and Access Management systems are important as entry points and ongoing contact points for FSA Trading Partners. Interactions with Trading Partners can establish effective communications channels that FSA can leverage for a variety of purposes.
- **Other FSA Initiatives** - Enrollment and Access Management must be coordinated with several other projects across FSA. This effort must also be coordinated with the FSA Security Architecture development work, RID and other Data Strategy projects, Integrated Partner Management responsibilities, Case Management Oversight efforts, and the PIN Site Reengineering project.

The business objectives and high-level requirements identified in this phase provide a foundation for future enrollment and access management solutions. The team will validate and prioritize the business objectives before identifying possible solution options. Based on the prioritized business objectives, Enrollment and Access Management will create a vision for an enterprise approach to enrolling and managing access for Trading Partners. Consolidating processes and tools will improve FSA control of critical enrollment and access management functions, increasing the efficiency of these processes and decreasing administrative costs. Most importantly, an enterprise approach will insulate Trading Partners from the complexities of the internal FSA enrollment and access management processes and improve the effectiveness of FSA service delivery.

Amendment History

DATE	SECTION/ PAGE	DESCRIPTION	REQUESTED BY	MADE BY
6/30/03	All	Document submitted for FSA-wide review.	N/A	R. Summers

Table of Contents

1 INTRODUCTION 8

1.1 BACKGROUND 8
1.2 OBJECTIVE AND DEFINITION OF TERMS 8
1.3 SCOPE 9
1.4 ORGANIZATION OF THIS DOCUMENT 10
1.5 APPROACH 11
1.6 INITIAL FINDINGS AND OBSERVATIONS 13

2 CURRENT STATE 15

2.1 INTRODUCTION 15
2.2 RELATIONSHIP BETWEEN ENROLLMENT AND ACCESS MANAGEMENT 15
2.3 METHODOLOGY 16
2.4 OVERVIEW OF CURRENT ACCESS MANAGEMENT PROCESSES 18
2.5 DETAILED PROCESS FLOWS - ACCESS MANAGEMENT 21
2.5.1 Process Flow – EZ Audit High Level Access Management 22
2.5.2 Process Flow – eCampus Based High Level Access Management 23
2.5.3 Process Flow – PEPS High Level Access Management 24
2.5.4 Process Flow – DCMS High Level Access Management 25

3 BUSINESS OBJECTIVES 26

3.1 INTRODUCTION 26
3.2 ACTIVITIES 26
3.3 BUSINESS OBJECTIVE FRAMEWORK 27
3.3.1 Description 27
3.3.2 Framework Sector Definitions 28
3.4 BUSINESS OBJECTIVES 30
3.5 BUSINESS OBJECTIVES DETAIL 31
3.5.1 Business Objective A1.1 – "Enterprise process focus" 32
3.5.2 Business Objective A2.1 – "Manage across systems" 33
3.5.3 Business Objective A2.2 – "Self-service capabilities" 34
3.5.4 Business Objective A2.3 – "Balance access and security" 35
3.5.5 Business Objective A2.4 – "Flexibility for future requirements" 37
3.5.6 Business Objective A2.5 – "User customization" 38
3.5.7 Business Objective A3.1 – "Streamline enrollment and registration" 39
3.5.8 Business Objective B1.1 – "Uniform process for access decisions" 40
3.5.9 Business Objective B2.1 – "Audit user access" 41
3.5.10 Business Objective B3.1 – "Meet regulatory requirements" 42
3.5.11 Business Objective C1.1 – "Facilitate enterprise access to data" 43
3.5.12 Business Objective C2.1 – "Enterprise policies and standards" 44
3.5.13 Business Objective C2.2 – "Security of FSA systems" 45
3.5.14 Business Objective C2.3 – "Match access privileges to job functions" 46
3.5.15 Business Objective C3.1 – "Effective training and customer support" 47
3.5.16 Business Objective C3.1 – "Adopt policies to improve processes" 48
3.6 BUSINESS INTEGRATION GROUP VISION FRAMEWORK CROSS REFERENCE 49

4 CONCLUSIONS AND NEXT STEPS 50

APPENDIX A: SECURITY DEFINITIONS OF ACCESS MANAGEMENT AND IDENTITY MANAGEMENT 53

APPENDIX B: BUSINESS OBJECTIVE MEETING SUMMARIES 55

APPENDIX C: QUESTIONNAIRES 56

APPENDIX D: BUSINESS INTEGRATION GROUP VISION FRAMEWORK 57

APPENDIX E: ENROLLMENT AND ACCESS MANAGEMENT BUSINESS OBJECTIVES VISION FRAMEWORK 58

Tables and Figures

Figure 1.1 – Information Gathering Sessions 12
Figure 2.1 – Enrollment and Access Management Relationship 16
Figure 2.2 – FSA Systems & Trading Partner Interaction 17
Figure 2.5 - Access Management User Types 18
Figure 2.6 – FSA System User, Action & Role Based Table 19
Figure 3.1 – Enrollment and Access Management Vision Framework 27
Figure 3.2 – Enrollment and Access Management Business Objectives 30
Figure 3.3 - Cross reference of Enrollment and Access Management Objectives with related Business Integration Group (BIG) Vision Framework Objectives. 49
Figure A1 - Security Functions and Processes That Comprise Access Management and Identity Management 54

1 Introduction

1.1 Background

The Department of Education's Office of Federal Student Aid (FSA) seeks improvements to data quality and data consistency. FSA is examining its overall approach to data to ensure accurate and consistent data exchange between customers, Trading Partners, and compliance and oversight organizations. FSA will also leverage a targeted data strategy to support program-wide goals of maintaining a clean audit and removing FSA from the GAO high-risk list.

Task Order 123 will define FSA's Enterprise Data Vision and its overall Enterprise Data Strategy. The end result of this task order will be an enterprise data framework that integrates the following components, addressing FSA's major data-related issues:

- FSA Data Strategy Framework
- Technical Strategies
- XML Framework
- Common Identifiers
- Enrollment and Access Management

Current enrollment and access management processes at FSA are very fragmented and complex. In addition, these processes have often been inconsistently implemented, particularly relating to access rights. The Enrollment and Access Management initiative will review FSA's current offerings for Enrollment and Access Management and document FSA's Business Objectives and High-Level Requirements. The high-level design will provide a roadmap for implementing a new vision.

Analysis and design activities for enrollment and access management are coordinated with RID and other Data Strategy projects. Integration of data collection and analysis work among these projects will provide a foundation for streamlining and simplifying Trading Partner enrollment and user access management across the enterprise.

1.2 Objective and Definition of Terms

The primary objective of the Enrollment and Access Management Team is to review and analyze FSA's current Enrollment and Access Management environment and look for ways to simplify these business processes for Trading Partners. The Enrollment and Access Management project was created in response to several key points:

- Currently, enrollment and access management processes and tools operate on a non-centralized, non-standardized basis. As a result, Trading Partner interactions with FSA systems are fragmented and complex.
- A simplified business process will reduce confusion among system-users relating to the hand-offs between Enrollment and Access Management.
- Processes for managing user access rights have often been inconsistently implemented.

For the purposes of this deliverable, *Enrollment* is defined to include both the Title IV enrollment certification process, which authorizes Trading Partners to participate in Title IV programs, and the initial registration of the Trading Partner's delegated administrator in various FSA systems. The term *registration* includes collection and processing of program and organization information to support approval, and the process of communicating the results of the eligibility decision to the Trading Partner. Registration does not include the eligibility decision process itself.

Access management is the term used to describe policies, processes, and tools that define user access privileges and roles; issue and approve user identity credentials that are linked to access privileges; and create, modify, audit, and remove user access to FSA systems. This definition includes processes and functions often referred to as "Identity Management" in the field of information security. Appendix A provides a more detailed discussion of the relationship between the term "access management" as used by the Enrollment and Access Management Team and the way this term is used by information security industry groups and product vendors.

Trading Partner is defined as all non-student groups that use FSA Systems. Trading Partners include post-secondary institutions (schools), other entities eligible to act on the behalf of schools, lenders, and audit and regulatory organizations. For the purposes of this deliverable, FSA staff and contractors are also included within the definition of Trading Partner.

1.3 Scope

This deliverable covers work defined in Task Order 123 related to documentation of Enrollment and Access Management Business Objectives and High-Level Requirements. The intent of the Enrollment and Access Management effort is to review and analyze FSA's current Enrollment and Access Management environment and look for ways to simplify the business process for Trading Partners. This effort will define the business objectives, high-level requirements, and high-level design for schools, other entities eligible to act on the behalf of schools, FSA staff, contractors, and audit and regulatory organizations in accessing FSA systems.

Deliverables 123.1.26 and 123.1.27 document the enrollment and access management business objectives and high-level requirements identified as a first step toward creating an updated enrollment and access management vision for FSA. Identifying specific solutions is not within the scope of this deliverable. The next phase of this project will consider solution options and develop a high-level design for enrollment and access management.

Several participants in this project noted examples of FSA policies and standards that may need to be created to support a new vision for enrollment and access management processes. Having the appropriate FSA security and privacy policies will be critical to successful deployment of an Enrollment and Access Management solution. Although the existing FSA security and privacy policies are not analyzed in detail in this deliverable, several of the high-level requirements do

address needs for policies and standards to cover specific topics related to enrollment and access management.

The information presented in this report was derived from existing FSA documentation and meetings with FSA personnel and contractors to define AS-IS processes. These resources were assumed to be subject matter experts in their given area and the information provided was assumed to be accurate and up to date. Validation and cross referencing of information was conducted as time permitted. The information provided by both participating Core Team members and the subject matter experts provided the primary input to produce the high level process flows, business objectives and conclusion contained within this document.

The business objectives and high-level requirements presented in this document are the suggestions and opinions of project participants. Objectives gathered during interviews and workshops will be considered for the target state but have not yet been categorized as final requirements. FSA business owners from a broad spectrum of organizations and business units identified several key business objectives that would help to simplify the enrollment and access management processes for Trading Partners. These business objectives and high-level requirements represent a combination of existing and desired functions and will need to be reviewed and updated to create an enterprise vision. Only after a detailed review, examination of potential gaps and barriers, and cost/benefit analysis, will the requirements list be finalized.

Some business objectives identified in this effort do not apply only to Enrollment and Access Management systems, but extend across the entire Data Strategy effort. Additional FSA enrollment and access management business objectives or high-level requirements may be defined through related system and application development efforts, as well as related projects that are part of the Data Strategy task order. These additional objectives and requirements will be integrated as appropriate into the FSA enrollment and access management vision.

1.4 Organization of This Document

This document, Deliverable 123.1.27, and the companion document, Deliverable 123.1.26, present the Enrollment and Access Management Business Objectives and High Level Requirements for Task Order 123. They contain a summary of work accomplished during the initial phase of this project, an overview of current Enrollment and Access Management processes currently employed at FSA, and the Business Objectives and High-Level Requirements gathered from FSA. The finalized list of Business Objectives and High Level Requirements will serve as an input to future High Level Design and visioning activities that are part of this Task Order.

The organization of this document is summarized below:

- Section 1 – *Introduction* discusses the context and background for the project and this deliverable.

- Section 2 – *Current State* examines the enrollment and access management processes currently employed at FSA. This section summarizes completed activities and analyzes existing processes.
- Section 3 – *Business Objectives* documents the Business Objectives and High-Level Requirements identified by FSA. This section defines Business Objectives and High-Level Requirements, reviews the framework used to group Business Objectives, and examines each Business Objective and example High-Level Requirement in greater detail.
- Section 4 – *Conclusions and Next Steps* describes recommended next steps for analyzing and integrating Business Objectives and High-Level requirements to create an FSA vision for the future. This vision will be documented in the Enrollment and Access Management High-Level Design.

The Task Order specifies that the Enrollment Business Objectives and High-Level Requirements and Access Management Business Objectives and High-Level Requirements be documented in separate deliverables. Deliverables 123.1.26 and 123.1.27 are organized as the Task Order specified, but the documents are closely related. Deliverable 123.1.26 contains business objectives and high-level requirements for FSA Enrollment. Because they are closely related, some business objectives apply to both Enrollment and Access Management. Short descriptions for business objectives that apply only to access management are included in Deliverable 123.1.26. Additional detail for the FSA Access Management business objectives and high-level requirements can be found in Deliverable 123.1.27.

1.5 Approach

The Enrollment and Access Management initiative is composed of two major phases. This first phase consists of business objective gathering and commenced on April 8, 2003. The next phase includes high-level designs and is to conclude November 17, 2003. Four major deliverables are planned:

- Deliverable 123.1.26 - Enrollment Business Objectives and High-Level Requirements. This deliverable documents FSA's business objectives and high-level requirements for providing integrated enrollment management for Trading Partners.
- Deliverable 123.1.27 – Access Management Business Objectives and High-Level Requirements. This deliverable documents FSA's business objectives and high-level requirements for providing Access Management for Trading Partners and FSA personnel in accessing FSA systems.
- Deliverable 123.1.28 – Enrollment High-Level Design. This deliverable (due on 11/17/03) will define the high-level design for providing an integrated enrollment management for Trading Partners.
- Deliverable 123.1.29 - Access Management High-Level Design. This deliverable (due on 11/17/03) will define the high-level design for providing integrated access management process for Trading Partners.

An initial Core Team project kickoff meeting was held on April 30, 2003. Eighteen information-gathering meetings were also held with Core Team members and system owners to understand and document current Enrollment and Access Management procedures for each system. The following chart summarizes the systems covered and the participants for the information gathering sessions:

System(s)	Participant(s)	Interview Date
CPS	Angeline Iwanicki	05/13/03
Participation Management SAIG	Gregory James, Paul Steinhauer	05/14/03
COD	Tony Milidantri, Ted Taverner/Renee Wade	05/15/03 05/20/03
FAA On-line	Nina Colon	05/15/03
Eapp PEPS	Jay Long, Chris Hill, Patricia Patterson	05/19/03
eCB	Rich Bennett, Tammy Connelly	05/20/03
DLSS	Randy Bowman, Allen Prodgers	05/20/03
DLDM	Randy Bowman, Allen Prodgers	05/20/03
eZAudit	Randy Wolff, Matt Portolese	05/21/03
CMDM	Andy Cho	05/21/03
NSLDS	Pam Eliadis, Andrea Wise	05/21/03
FMS - Core App FMS – LaRS FMS – LAP FMS - GAFR	Stephen Mallack, Pamela Jefferson, Matt Fontana, Angela Baker, Frank Ramos	05/22/03
FPDM	Nettie Harding	05/22/03
Schools Portal	Colleen Kennedy	05/28/03
IFAP	Colleen Kennedy	05/28/03
Collections (DMCS)	Gregory Plenty, Courtland Smith, Steve Martus	05/29/03
Consolidation (DLCS)	Denise Leifeste, Bill Burns, David Yang	05/30/03
FMS - LEAP/SLEAP	Greg Gerrans	06/06/03

Figure 1.1 – Information Gathering Sessions

Additional information on the Information Gathering Participants and meeting summaries are presented in Appendix C – Questionnaires.

An iterative approach was employed to identify and validate sample business objectives. Initial business objectives were drafted from the Business Integration Group's general security objectives, the overall data strategy effort business objectives sessions, and individual information-gathering sessions held with the Core Team members and system owners. Next, all of those Business Objectives were organized according to the Business Integration Group (BIG) Vision Framework. Finally, three group meetings were held with representatives from the areas of Delivery and Eligibility, Servicing, and Applications during the week of June 9–13, 2003. The Business Objective meeting participants and meeting summaries are in Appendix B – Business Objective Meeting Summaries. In each meeting the sample business objectives were reviewed and validated. Additional business objectives were also identified and documented. After each meeting the business objectives were summarized and analyzed. Finally, the Business Objectives were discussed and validated during a Core Team meeting on June 25, 2003.

Upon completion of this deliverable, the Enrollment and Access Management Team will proceed with work in the next phase of the initiative, high-level design.

1.6 Initial Findings and Observations

Detailed Enrollment and Access Management findings are described in Section 3 – Business Objectives. However, several overall findings and observations were made during the process of conducting information-gathering sessions and analyzing the business objective and high-level requirements. These general findings and observations are summarized below:

- **Current FSA enrollment and access management processes are very complex.** As demonstrated in the analysis of the current state, there are many points of confusion for users about system responsibilities and access procedures. For example, many users refer to SAIG as the system that manages participation to a group of FSA systems. However, SAIG primarily manages the exchange of files. It is the Participation Management system (PM) that manages Data Point Administrator (DPA) sign-up for a selected group of systems, including SAIG. The perception that it is SAIG that manages the sign-up process may confuse users trying to request access to other systems. *Future business processes should insulate Trading Partners from the underlying complexities of FSA system interactions.*
- **Enrollment and Access Management solutions will require integration across policies, processes, and technologies.** Discussions about business objectives and high-level requirements for enrollment and access management touched on a variety of FSA operational processes, policies, and technologies. These discussions highlighted the fact that the future vision for enrollment and access management must support an integrated set of solutions in line with FSA business goals. No single technology or process change will be able to meet all objectives.
- **Enrollment and Access Management should be considered from an enterprise perspective.** Most enrollment and access management processes currently operate on a system-by-system basis. Many participants articulated a need to focus on processes and solutions at the enterprise level. An enterprise approach to enrollment and access

management will also result in streamlined processes, increased efficiency, reduced costs, improved handling of enrollment and access management data, and improved services to Trading Partners.

- **Enrollment and Access Management objectives will need to be prioritized**. FSA business objectives for enrollment and access management represent a wide range of capabilities that will need to be prioritized during later phases of this project. Some business objectives reflect current business processes. Other objectives described new processes and functions that do not currently exist. Such new capabilities may involve reengineered processes or the development of new technical solutions. They will need to be analyzed for feasibility since they may require substantial effort to define and implement.
- **Enrollment and Access Management will be enabling systems for some FSA objectives**. Not all the FSA business objectives identified were confined to single functional areas, and several extend beyond the boundaries of the Enrollment and Access Management project. Some of the business objectives identified are functions or processes that Enrollment and Access Management must support, but are not capabilities that would be directly deployed as part of enrollment and access management systems. For example, user personalization functions are usually implemented within systems and applications, although they will need to exchange identity information with enrollment and access management systems. The business objectives defined during this project must be coordinated with other FSA efforts to provide the appropriate context for design and integration.
- **Enrollment and Access Management systems will need to integrate with FSA Security and Privacy Policy.** Several security and privacy efforts are under way within FSA. The FSA Information Technology Security and Privacy Policy effort provides a foundation for future information security and privacy guidelines, standards, processes, and procedures. The Security Architecture initiative developed a proposed FSA Security and Privacy Architecture vision consisting of security services, technical components, and standards to guide planning and development for security across FSA. The Enrollment and Access Management effort will need to document security and privacy policy implications and coordinate them with the FSA security organization during system design and development phases.
- **Other FSA initiatives will affect the design of enrollment and access management capabilities.** Planning for Enrollment and Access Management solutions will clearly depend on other Security and Data Strategy project initiatives. In addition, Enrollment and Access Management has a variety of potential integration points with other FSA projects including Case Management Oversight (CMO), PIN Site Re-engineering (PIN), Integrated Partner Management (IPM), and Common Services for Borrowers (CSB). These efforts will need to be consulted during the upcoming high-level design phase.

2 Current State

2.1 Introduction

Currently, the FSA portfolio of applications consists of 21 systems that Trading Partners use to originate, disburse, collect, and manage Title IV Financial Aid for students. These 21 applications provide services to Trading Partners and do not include all FSA systems (e.g. FSA internal systems). This environment has grown in complexity over the years. It is hosted on five different hardware platforms and runs on four different application servers located in multiple data centers. Trading Partner systems are operated by eight separate contractors, and are supported 11 help desk and customer care centers. Needless to say, it has become difficult for Trading Partners to do business with FSA. Likewise, it has become difficult for FSA to manage Trading Partner access across these systems.

Some Trading Partners have as many as 10 separate user names and passwords, and must log on to each application separately to obtain cross-system information. Even a relatively simple process, like resetting passwords, can be confusing because of the number of systems involved and the different methods that apply to each system. From an FSA perspective, managing user access on a system-by-system basis has become expensive and unwieldy. As Trading Partners add, terminate, and change individual users and roles within their organizations, the burden of properly tracking user permissions across applications is a growing challenge. This also means that the risk of allowing unauthorized access to FSA data increases as new systems are added.

2.2 Relationship Between Enrollment and Access Management

The current FSA environment is very complex and includes many entry points through which Trading Partners can access FSA data. The process of approving individual users and then authorizing them to access FSA data varies greatly depending on the type of Trading Partner and the data that is being accessed. The variability in processes and terminology used in the current FSA environment make it difficult to determine the exact boundary between the enrollment and access processes. For the purpose of this analysis, the Enrollment and Access Management Team decided that the process of enrollment includes Trading Partner enrollment in Title IV programs, and the initial registration of the designated administrator. The access management process is considered to begin when the designated administrator starts processing individual user requests for access to FSA systems. The diagram below (Figure 2.1) shows this interaction between enrollment and access management and emphasizes their close relationship. The enrollment and access management processes will be discussed separately in the following sections.

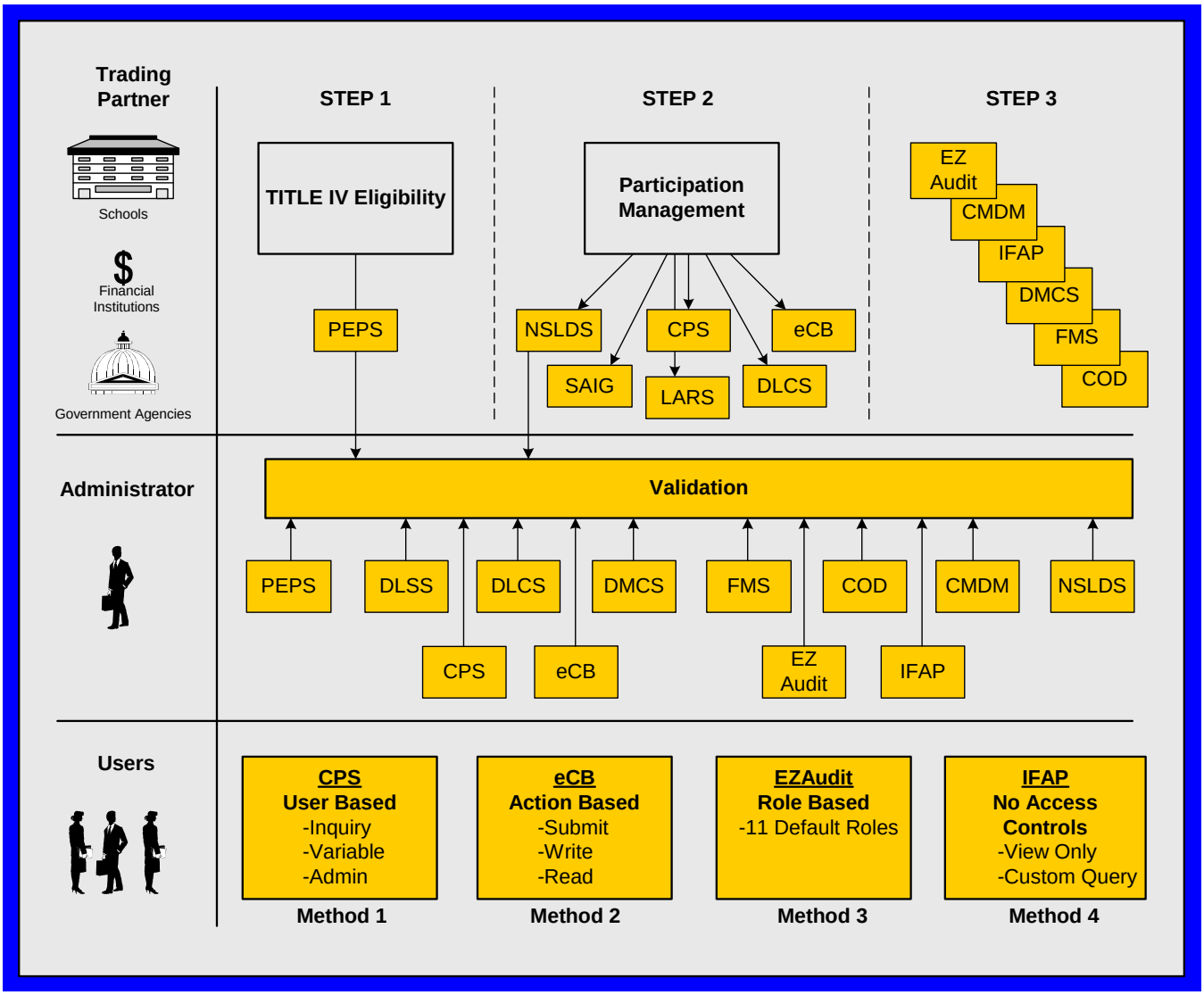


Figure 2.1 – Enrollment and Access Management Relationship

2.3 *Methodology*

The first step in the analysis of existing enrollment and access management processes was to gather information about the current system enrollment and access methods for each FSA system. To capture this current state information, a detailed questionnaire was developed and distributed to application subject matter experts identified by FSA. These contacts are listed in the table shown in Section 1.4. Individual meetings were then conducted with each application expert to complete the questionnaire. The questionnaires were pre-populated with information gained from preliminary research of FSA application websites and Integration Partner resources. This preliminary work enabled the access and enrollment team to become familiar

with each application's enrollment and access management processes. More importantly, this research allowed the team to validate existing information and to ensure that individual application meetings would be as productive as possible. Following each application meeting the questionnaires were updated then redistributed to the application experts for review and feedback. Appendix C of this deliverable contains copies of the completed questionnaires.

Information from the questionnaire about the users or Trading Partners needing access to each system is shown in Figure 2.2. This figure shows the systems each Trading Partner uses to do business with FSA. Noted in the right-hand column is the total number of systems required for each Trading Partner. Readily apparent is the complex nature of FSA systems and the variety of interactions required for each Trading Partner. The number of systems required by each Trading Partners varies; Postsecondary Institutions (schools), 3rd party services, customer service representatives, and guarantee agencies use as many as 10 systems each, while lenders, Private Collection Agencies (PCAs) and Federal and State agencies use five systems or less. Note that although the table shows that all 21 systems are available to internal FSA users and contractors, but a single individual user would not typically need access to that many systems. Further analysis across business functions within FSA will be needed to determine which groups of FSA users require access to multiple systems.

	FSA Systems																				
	Title IV		Participation Management							Other Systems											
Enrollment & Access Management	PEPS (eAPP)	SAIG	FAA Access On-line	CPS	eCB	DLSS - eServicing/non-Student	NSLDS - Non-Student	FMS - LARS	Delinquent Loans Datamart	COD	EZ Audit	Credit Management Datamart	FMS	FMS - GAFR	FMS - LEAP/SLEAP	FPDM	Schools Portal	IFAP	DMCS	DLCS - Non-Student	PIN	Totals
Trading Partners																					
Post Secondary Institutions		•	•	•	•		•			•	•						•	•				10
3rd Party Servicers	•	•	•	•	•		•			•	•						•	•				10
Internal FSA Users/Contractors	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	21
Customer Service			•	•	•	•	•			•							•	•	•	•		10
Guarantee Agencies	•	•		•			•	•						•		•	•	•				9
PCA's																			•			1
State Agencies	•	•					•										•	•				5
Federal Agencies		•															•	•				3
Lenders		•				•	•	•												•		5
Others					•																	1

Figure 2.2 – FSA Systems & Trading Partner Interaction

2.4 Overview of Current Access Management Processes

The Access Management process controls the approval, assignment, and management of access privileges for users of FSA systems. Access control functions limit the systems and operations available to users, and enforce policies that define the allowable actions of authorized users. Access management and control systems protect the confidentiality and integrity of FSA applications, systems, and information. Access management relies upon the accurate identification and authentication of each user to create a tight association with the privileges assigned to an individual. Refer to Appendix A for an additional discussion of the relationship between "access management" as used here and general security concepts such as "access control."

Access to FSA systems is currently managed on a system-by-system basis, with the exception of the PM/SAIG system that manages file exchange access for several applications. Typically, user access accounts are provisioned, configured, and modified by processes and administrators that cover individual systems. Each system adopts its own rules and procedures to manage user access.

Of the 21 Trading Partner systems, most can be classified into three general categories based on the mechanism implemented to control user access. These methods are: User Based access, Action Based access, and Role Based access. A fourth grouping of FSA systems was created to categorize those applications that did not have an access management system or could not be classified into one of the above categories. Examples of FSA systems that fit into these categories are depicted in Figure 2.5. The three major methods used by FSA to control access are described in subsequent paragraphs.

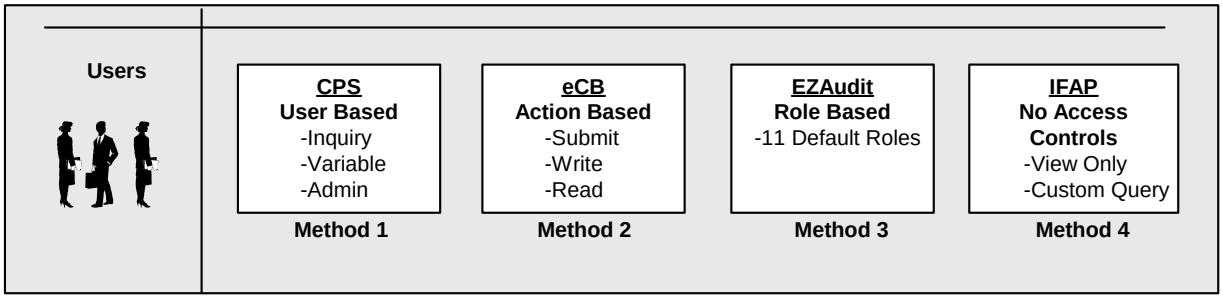


Figure 2.5 - Access Management User Types

User Based Access Control: User based access control is the ability to control or restrict access based upon username. A separate list of access privileges (an Access Control List) is maintained by the system for each user. This is a fairly traditional approach for user access and is usually most effective in a static environment. The administration of this type of systems becomes difficult to manage when an environment is dynamic and users join or leave the organization frequently, or change positions within an organization. Of the 21 systems reviewed, seven FSA systems had a user based access method.

Action Based Access Control: Action Based control does not restrict users to particular data, but rather restricts the functions that an individual user can perform. An example of this approach is to allow certain users to have only the ability to read information, without the ability to change it (i.e., assigning a 'read' privilege instead of a 'read- write' privilege). This is a fairly basic method of controlling user access. Although it is much simpler to manage than the user based assess methods, it does not provide a great deal flexibility for controlling access to diverse types of information. Two FSA systems use this method of access control.

Role Based Access Control: Role Based access control is a relatively new approach that maps access privileges to organizational responsibilities. In this system, user roles are defined that correspond to a set of access privileges appropriate for a specific type of user or job function. When a user is connected to a role, the system confers on the user all the access privileges associated with that role. This approach improves security, by increasing the accuracy of privileges assigned to each user, and reduces administrative costs, by reducing the effort required to configure access for each user access to individual applications, data sets, and other system resources. By assigning individuals to predefined roles, the administrative process of establishing privileges is streamlined and management time for reviewing privilege assignments can be reduced. Security can also be improved by preventing users from obtaining inconsistent or incompatible privileges. Only one FSA system currently uses this method. The real advantage of Role Based Access Control would be to extend this concept to create an enterprise role capability across all FSA systems.

User Based	Action Based	Role Based	Other
COD	CPS	EZ-Audit	FMS – LEAP/SLEAP
DLCS	eCB		PM/SAIG
DMCS (RACF)			IFAP
DLSS			Schools Portal
FMS – GAFR			
FMS – LAP, LARS			
FPDM			
NSLDS (RACF)			
FAA Online			
PEPS			

Figure 2.6 – FSA System User, Action & Role Based Table

In addition to the direct user based access control methods, data can be exchanged between Trading Partners and FSA applications through the Student Aid Internet Gateway (SAIG).

SAIG allow schools to perform record updates to several systems by utilizing a PC based software package called EDExpress. EDExpress consists of four software modules. They are Application Processing, Packaging, Direct Loan, and Pell.

The Application Processing module allows users to enter, report, and manage all Title IV student financial aid application information by receiving data from the CPS via SAIG and reformatting and storing it in a local EDExpress database. The Financial Aid Administers can then update application data, calculate an estimate EFC and resolve edit failures. The changes can then be batched and transmitted back to the CPS. All permissions and data assess management functions are handled by SAIG.

The Packaging module contains all the basic activities included in tracking and awarding students Title IV federal aid, state aid, institutional aid, and aid from other outside resources. The same data collected in the Application Processing module can be used to create an electronic award package for a student.

The Direct Loan module allows schools, with valid SAIG TG Numbers, to exchange loan origination, print request, disbursement, reconciliation, and enrollment status records with the Direct Loan Origination Center. Requests for Direct Loan funding are transmitted through the SAIG to the Direct Loan Servicing Center.

The Pell Payment module provides tools to create, edit, and report Pell Payment Origination and Disbursement data. Users can import either ISIR or packaging data. Once this Pell Payment data has been entered or imported, it can be exported and transmitted electronically to the Recipient Financial Management System (RFMS) via SAIG. Pell Payment data is processed by RFMS and returned to the schools SAIG destination point mailbox.

2.5 Detailed Process Flows - Access Management

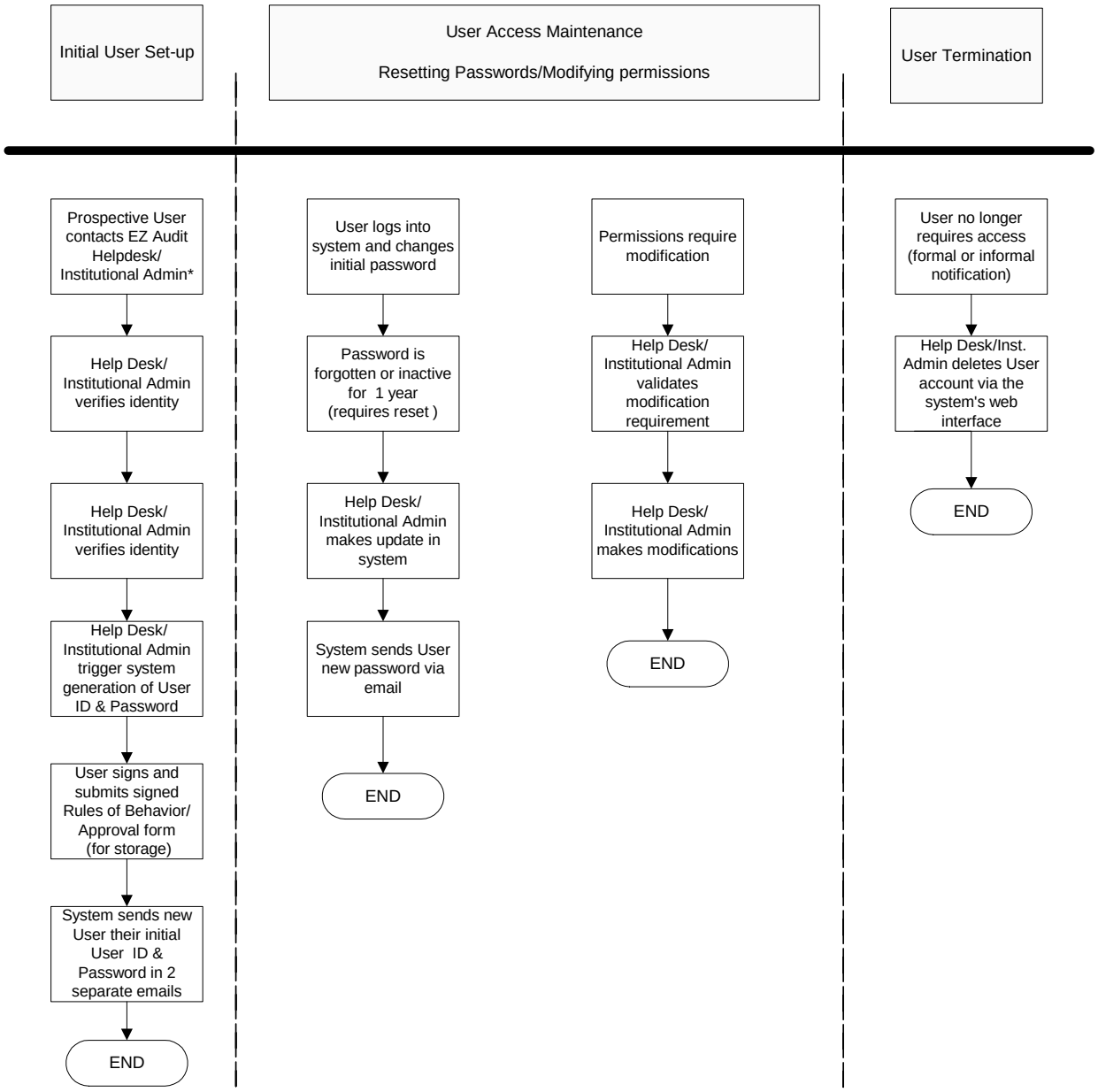
Regardless of the method used to control user access, several administrative functions are required by each system. These administrative functions include:

- Set-up of user accounts and initial configurations
- Set-up initial user name and password (credentials)
- Communication of credential to user
- Modification of user permissions
- Resetting passwords
- Termination of users

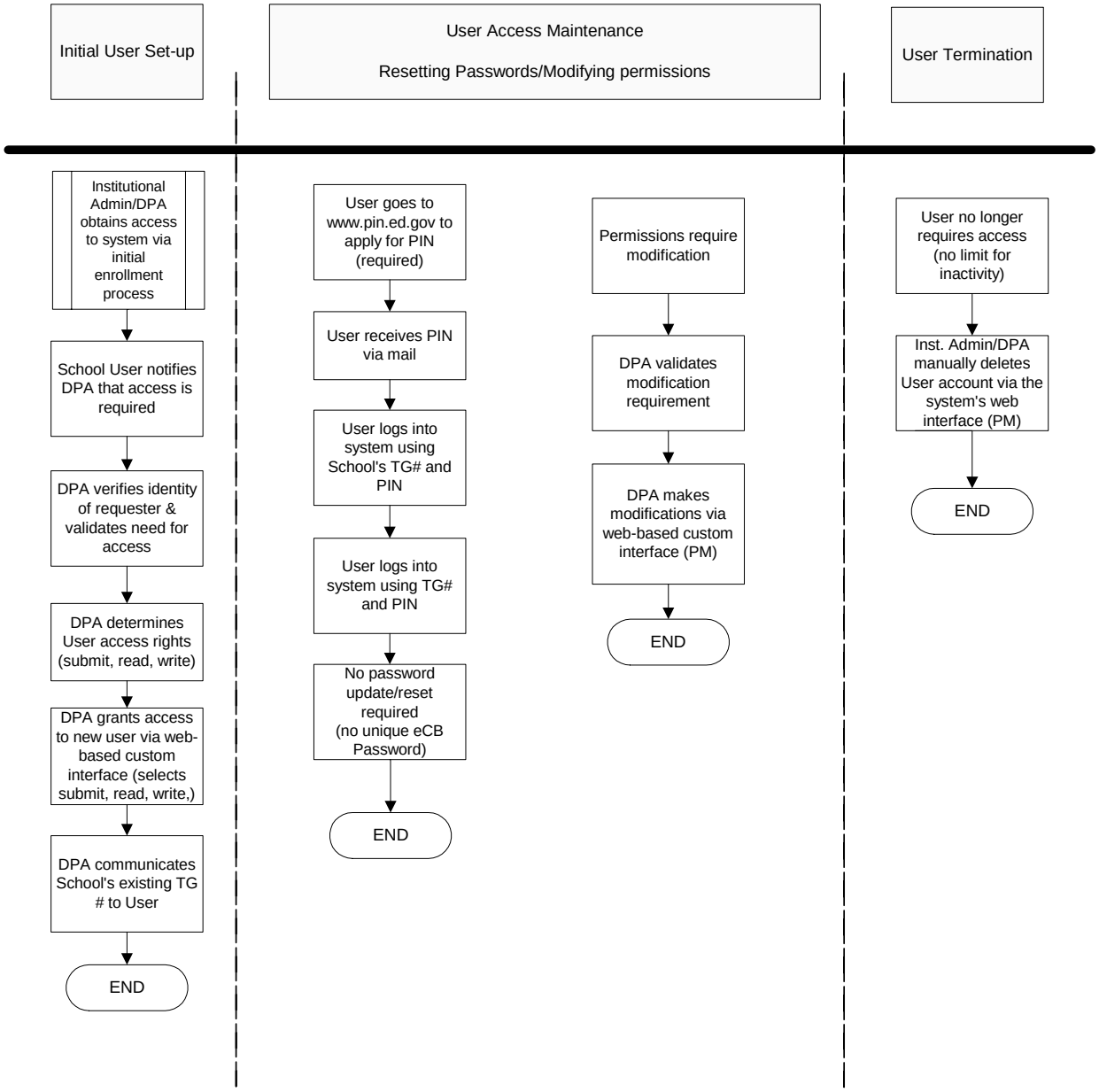
Sample process flows for these functions from representative system are presented below. Although the processes are fairly simple, managing each process separately for 21 different systems is both expensive for FSA and confusing for the end users. A centralized system or tool that can be used to configure access across multiple FSA systems, and a centralized means of viewing or displaying access rights across the enterprise, would reduce administrative costs and provide functional benefits to FSA users.

Additional process flows for individual application will be developed as needed during subsequent phases of the Access Management effort.

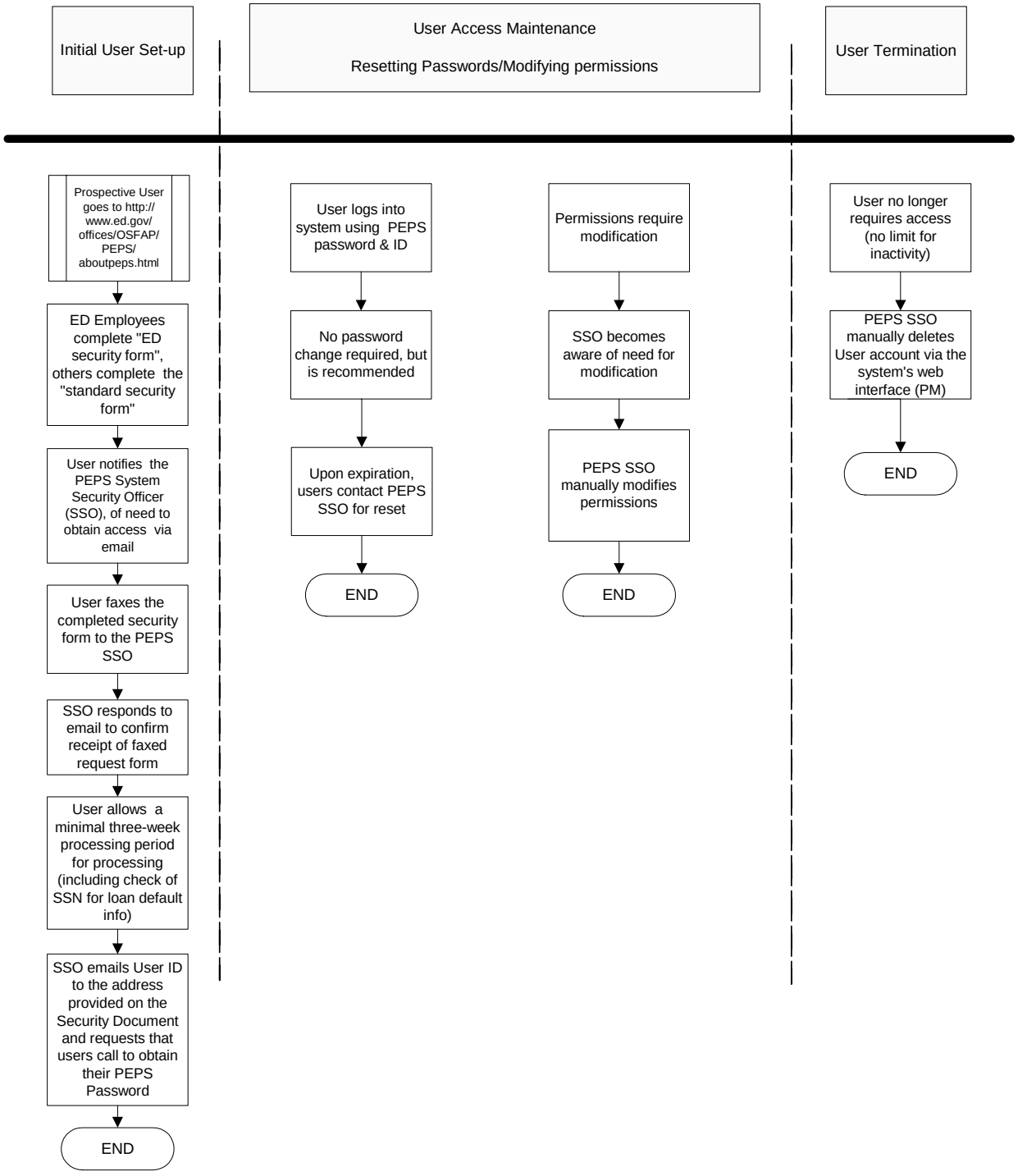
2.5.1 Process Flow – EZ Audit High Level Access Management



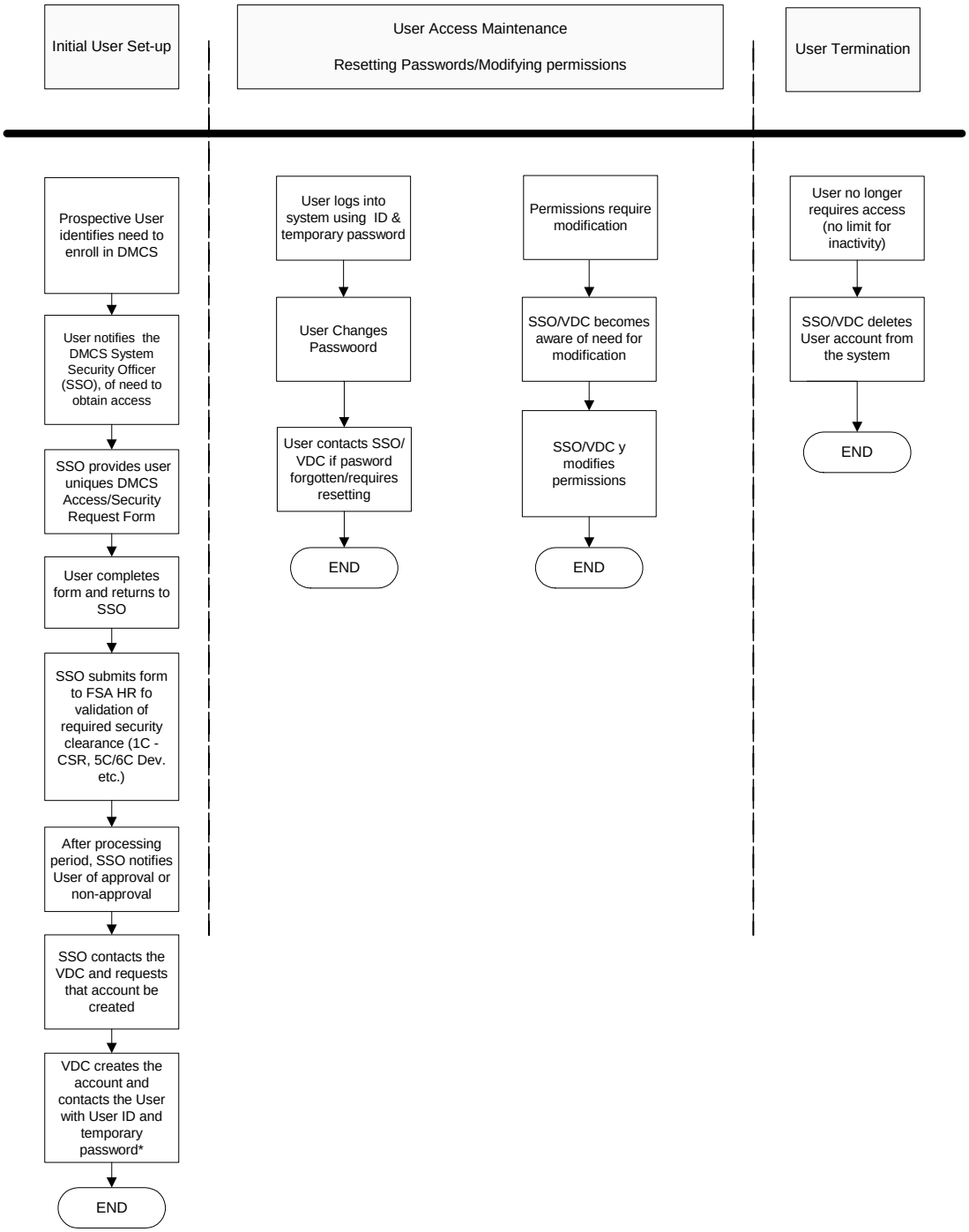
2.5.2 Process Flow – eCampus Based High Level Access Management



2.5.3 Process Flow – PEPS High Level Access Management



2.5.4 Process Flow – DCMS High Level Access Management



* In some circumstances, the regional office SSO facilitates the user ID process.

3 Business Objectives

3.1 Introduction

Business Objectives are a statement of purpose to help the enterprise define a vision for future efforts. They provide high-level direction and standards for complex enterprise issues. Business Objectives are not high-level requirements and do not specify a design or dictate a solution.

High-level requirements are created in the planning stage of a project and provide more detail than business objectives. High-level requirements are not detailed requirements or a design. High-level requirements also do not dictate a solution but provide examples and clarifications for the business objective. More detailed requirements must be identified before beginning detailed design activities.

3.2 Activities

An iterative approach was employed to identify and validate the enrollment and access management business objectives. Sample business objectives were initially created based on the individual information-gathering sessions held with the Core Team members and system owners. Those Business Objectives were organized into the Business Integration Group (BIG) Vision Framework structure. An example of the BIG Vision Framework is shown in Appendix D. Three group meetings were held with representatives from the Delivery and Eligibility, Servicing, and Applications areas to identify, review, validate, and document enrollment and access management business objectives. Additional detail on these meetings is in Appendix B – Meeting Summaries. After each meeting the Business Objectives were summarized and analyzed. The revised business objectives were discussed and validated with the Core Team.

3.3 Business Objective Framework

3.3.1 Description

The Enrollment and Access Management Vision Framework below was used to group and examine business objectives and high-level requirements. This framework is based on the Business Integration Group (BIG) Vision Framework. While the enterprise vision framework was used to create this structure, the Enrollment and Access Management Business Objectives are at a much more detailed level specific to tools, processes, and functional areas for enrollment and access management. Please see section 3.6 for a mapping of Enrollment and Access Management Business Objectives to the BIG Vision Framework objectives.

		Core Business Outcomes		
		Provide Easier Access to Make it Easier for Our Customers to do Business With Us **A. "Easier Access"**	**Maintain Right & Effective Levels of Oversight Through Combination of Enhanced Tools & Customer Self-Monitoring** **B. "Effective Oversight"**	**Run the Business to Enable Right Actions, Right Transactions to the Right People** **C. "Right Transactions to the Right People"**
Core Business Enablers	**Support Effective & Informed Decision Making by Making the Right Information Available at the Right Time to the Right People** **1. "Effective Decision Making"**	A1.1 - Focus on registration processes and access decisions at the enterprise level instead of on a per system basis.	B1.1 - Adopt a uniform decision making process for evaluating users requesting access to FSA systems.	C1.1 - Facilitate access to sets of data at the enterprise level.
	Provide the Right Security, Tools, Systems, Architecture & Technology to Enable the Business to Achieve its Outcomes **2. "Right Tools & Technology"**	A2.1 - Manage enrollment and access privileges at the enterprise level.	B2.1 - Provide effective oversight of user access to FSA systems.	C2.1 - Create enterprise policy and standards for enrollment and access management.
		A2.2 - Improve self-service capabilities.		C2.2 - Maintain security of FSA systems.
		A2.3 - Balance easier access and system security.		C2.3 - Provide users with access to FSA systems appropriate for their job function.
		A2.4 - The enrollment and access solution should be flexible enough to support the requirements of current and future FSA systems.		
		A2.5 - Allow users to customize their experience with FSA systems.		
	Improve & Integrate Business Processes Into Delivery Solutions **3. "Improve Business Process"**	A3.1 - Streamline enrollment and access management for Trading Partner services.	B3.1 - Meet FSA regulatory compliance requirements.	C3.1 - Provide effective training and customer support across FSA systems.
				C3.2 - Adopt enrollment and access management policies that improve business processes.

Figure 3.1 – Enrollment and Access Management Vision Framework

	Enrollment and Access Management Business Objective
	Access Management Only Business Objective
	Cross-Team Business Objective

3.3.2 Framework Sector Definitions

A1: "Easier Access" and "Effective Decision Making"

Sector A1 captures business objectives that relate to the BIG Integration Vision Framework outcomes "Provide Easier Access to Make it Easier for Our Customers to do Business With Us" and "Support Effective & Informed Decision Making by Making the Right Information Available at the Right Time to the Right People."

A2: "Easier Access" and "Right Tools and Technology"

Sector A2 captures business objectives that relate to the BIG Integration Vision Framework outcomes "Provide Easier Access to Make it Easier for Our Customers to do Business With Us" and "Provide the Right Security, Tools, Systems, Architecture & Technology to Enable the Business to Achieve its Outcomes."

A3: "Easier Access" and "Improve and Integrate Business Processes"

Sector A3 captures business objectives that relate to the BIG Integration Vision Framework outcomes "Provide Easier Access to Make it Easier for Our Customers to do Business With Us" and "Improve & Integrate Business Processes Into Delivery Solutions."

B1: "Effective Oversight" and "Effective Decision Making"

Sector B1 captures business objectives that relate to the BIG Integration Vision Framework outcomes "Maintain Right & Effective Levels of Oversight Through Combination of Enhanced Tools & Customer Self-Monitoring" and "Support Effective & Informed Decision Making by Making the Right Information Available at the Right Time to the Right People."

B2: "Effective Oversight" and "Right Tools and Technology"

Sector B2 captures business objectives that relate to the BIG Integration Vision Framework outcomes "Maintain Right & Effective Levels of Oversight Through Combination of Enhanced Tools & Customer Self-Monitoring" and "Provide the Right Security, Tools, Systems, Architecture & Technology to Enable the Business to Achieve its Outcomes."

B3: "Effective Oversight" and "Improve and Integrate Business Processes"

Sector B3 captures business objectives that relate to the BIG Integration Vision Framework outcomes "Maintain Right & Effective Levels of Oversight Through Combination of Enhanced Tools & Customer Self-Monitoring" and "Improve & Integrate Business Processes Into Delivery Solutions."

C1: "Right Transactions to the Right People" and "Effective Decision Making"

Sector C1 captures business objectives that relate to the BIG Integration Vision Framework outcomes "Run the Business to Enable Right Actions, Right Transactions to the Right People" and "Support Effective & Informed Decision Making by Making the Right Information Available at the Right Time to the Right People."

C2: "Right Transactions to the Right People" and "Right Tools and Technology"

Sector C2 captures business objectives that relate to the BIG Integration Vision Framework outcomes "Run the Business to Enable Right Actions, Right Transactions to the Right People" and "Provide the Right Security, Tools, Systems, Architecture & Technology to Enable the Business to Achieve its Outcomes."

C3: "Right Transactions to the Right People" and "Improve and Integrate Business Processes"

Sector C3 captures business objectives that relate to the BIG Integration Vision Framework outcomes "Run the Business to Enable Right Actions, Right Transactions to the Right People" and "Improve & Integrate Business Processes Into Delivery Solutions."

3.4 Business Objectives

Listed below is the entire set of the Enrollment and Access Management Business Objectives:

Number	Business Objective
A1.1	Focus on registration processes and access decisions at the enterprise level instead of on a per system basis.
A2.1	Manage enrollment and access privileges at the enterprise level.
A2.2	Improve self-service capabilities.
A2.3	Balance easier access and system security.
A2.4	The enrollment and access solution should be flexible enough to support the requirements of current and future FSA systems.
A2.5	Allow users to customize their experience with FSA systems.
A3.1	Streamline enrollment and access management for Trading Partner services.
B1.1	Adopt a uniform decision making process for evaluating users requesting access to FSA systems.
B2.1	Provide effective oversight of user access to FSA systems.
B3.1	Meet FSA regulatory compliance requirements.
C1.1	Facilitate access to sets of data at the enterprise level.
C2.1	Create enterprise policy and standards for enrollment and access management.
C2.2	Maintain security of FSA systems.
C2.3	Provide users with access to FSA systems appropriate for their job function.
C3.1	Provide effective training and customer support across FSA systems.
C3.2	Adopt enrollment and access management policies that improve business processes.

Figure 3.2 – Enrollment and Access Management Business Objectives

3.5 Business Objectives Detail

For ease of reference, the business objectives and high-level requirement details are documented in a uniform format. The fields of the detail matrix are defined in the following example:

Scope:	This field indicates whether the business objective relates to Enrollment, Access Management, or both.	
Identifier/Title:	XX.X - Statement of business objective.	
Description:	Provides full description and supporting details for the business objective.	
High-Level Requirements:	XX.X.1	High-level requirement #1 – Statement of high-level requirement.
	XX.X.2	High-level requirement #2 – Statement of additional requirements, etc.
Additional Information	Provides supplementary details, assumptions, examples, and business context for the high-level requirements.	

This document presents business objective and high-level requirement details for FSA access management and is meant as a companion deliverable to 123.1.26 Enrollment Business Objectives and High-Level Requirements. For the reader's convenience, the enrollment business objective deliverable contains placeholders and short descriptions for enrollment business objectives. However, additional detail on Enrollment Business Objectives and High Level Requirements is located in Deliverable 123.1.26.

3.5.1 Business Objective A1.1 – "Enterprise process focus"

Scope:	Enrollment and Access Management
Identifier/Title:	A1.1 - Focus on registration processes and access decisions at the enterprise level instead of on a per system basis.
Description:	Refer to Deliverable 123.1.26 Enrollment Business Objectives and High-Level Requirements.

3.5.2 Business Objective A2.1 – "Manage across systems"

Scope:	Enrollment and Access Management
Identifier/Title:	A2.1 - Manage enrollment and access privileges at the enterprise level.
Description:	Refer to Deliverable 123.1.26 Enrollment Business Objectives and High-Level Requirements.

3.5.3 Business Objective A2.2 – "Self-service capabilities"

Scope:	Enrollment and Access Management
Identifier/Title:	A2.2 - Improve self-service capabilities.
Description:	Refer to Deliverable 123.1.26 Enrollment Business Objectives and High-Level Requirements.

3.5.4 Business Objective A2.3 – "Balance access and security"

Scope:	Access Management	
Identifier/Title:	A2.3 - Balance easier access and system security.	
Description:	Make enrollment and access management easier for Trading Partners to the extent that is consistent with FSA security objectives and regulatory requirements. Develop policies, processes, and tools that define and implement a balanced approach that minimizes barriers to access yet appropriately protects FSA systems and data.	
High-Level Requirements:	A2.3.1	Mitigate risk of single access point to the Title IV Aid Delivery process.
	A2.3.2	Provide business continuity processes that allow easy recovery of access management systems.
	A2.3.3	Provide session timeout features that balance usability with FSA security requirements.
	A2.3.4	Minimize restrictions on public information.
Additional Information	A2.3.1 – In the interest of making access to FSA systems easier, enrollment and access management systems may be consolidated. This may introduce single points of failure into the FSA environment. Whenever enrollment or access management processes are consolidated into single points of contact or single processing streams, redundancy and backup tools and processes should be provided to support continuity of operations in the event of system outages, failures, or other events that affect system availability. A2.3.2 – Business operations should be quickly recoverable in the event that access management systems are compromised or fail, whether because of accidental events (disasters, operational failures, exceeding system capacity) or intentional acts (such as Denial of Service (DoS) attacks). A2.3.3 – Some users complain about the session timeout feature that requires a user to login after a certain period of inactivity. This function is a security control that limits unauthorized use of systems in the event a user leaves a work station logged in. FSA systems should adhere to a consistent policy for session timeout that balances usability (and user annoyance) with FSA security requirements. A2.3.4 – Information that is public or not sensitive should not be restricted or require intrusive controls on access. For example, public FSA information should not require a user to log in to a system to obtain access, or a user should be able to view the data through a	

	'Guest' or 'Anonymous' account.

3.5.5 Business Objective A2.4 – "Flexibility for future requirements"

Scope:	Enrollment and Access Management
Identifier/Title:	A2.4 - The enrollment and access solution should be flexible enough to support the requirements of current and future FSA systems.
Description:	Refer to Deliverable 123.1.26 Enrollment Business Objectives and High-Level Requirements.

3.5.6 Business Objective A2.5 – "User customization"

Scope:	Data Strategy
Identifier/Title:	A2.5 - Allow users to customize their experience with FSA systems.
Description:	Refer to Deliverable 123.1.26 Enrollment Business Objectives and High-Level Requirements.

3.5.7 Business Objective A3.1 – "Streamline enrollment and registration"

Scope:	Enrollment and Access Management
Identifier/Title:	A3.1 - Streamline enrollment and access management for Trading Partner services.
Description:	Refer to Deliverable 123.1.26 Enrollment Business Objectives and High-Level Requirements.

3.5.8 Business Objective B1.1 – "Uniform process for access decisions"

Scope:	Access Management	
Identifier/Title:	B1.1 - Adopt a uniform decision making process for evaluating users requesting access to FSA systems.	
Description:	Different systems currently perform different eligibility verification checks during enrollment and registration processes. A uniform process for evaluating and processing access requests would provide a more consistent decision about eligibility.	
High-Level Requirements:	B1.1.1	Provide the capability to review default and overpayment records.
	B1.1.2	Enable access decisions at the business process level.
Additional Information	The verification process should include standard checks for situations that would affect eligibility or access approvals. Examples of checks that should be uniformly applied across all systems include: • Default status • Debarments • Criminal convictions.	

3.5.9 Business Objective B2.1 – "Audit user access"

Scope:	Access Management	
Identifier/Title:	B2.1 - Provide effective oversight of user access to FSA systems.	
Description:	Security policy defines rules and procedures to safeguard the enterprise. In order for those policies to be success, the policies must be strictly enforced. An effective access management system must provide effective oversight of user access to FSA systems by ensuring compliance with FSA Enterprise Security Policies.	
High-Level Requirements:	B2.1.1	Provide the ability to efficiently identify accounts that should be removed or disabled.
	B2.1.2	Provide a convenient, effective way to view and report on access privileges of users across multiple systems.
	B2.1.3	Provide an audit trail sufficient to track updates and perform historical research.
	B2.1.4	Provide ability to view user access privileges over time.
	B2.1.5	Provide automated procedures to identify anomalies in access or inappropriate combinations of access privileges across systems.
	B2.1.6	Support consolidated reporting on enrollment and access management across FSA systems.
Additional Information	These high-level requirements are examples of ways that effective oversight can be achieved. An important opportunity that is gained by an enterprise view of users' system access is the ability to achieve a holistic view of an individual's access to the enterprise. In order to take advantage of this opportunity, an access management system must provide views and reports on individual access for each system. In the event that additional research is necessary, audit trails that record user activity will facilitate additional information gathering. Ideally, automated procedures will assist manual efforts in the oversight process. Complex rules for appropriate and inappropriate access must be defined in order for automated procedures to be effective. Currently, an issue that was revealed in Business Objective meetings described related to Financial Aid Administrations (FAAs) who leave an institution. Due to the nature of many systems, FSA is currently dependent on users or their institution to report their departure to FSA so their access can be properly terminated. It is possible that access could be retained through lack of communication. Proper procedures and tools to identify accounts for removal is a must for effective oversight.	

3.5.10 Business Objective B3.1 – "Meet regulatory requirements"

Scope:	Enrollment and Access Management
Identifier/Title:	B3.1 - Meet FSA regulatory compliance requirements.
Description:	Refer to Deliverable 123.1.26 Enrollment Business Objectives and High-Level Requirements.

3.5.11 Business Objective C1.1 – "Facilitate enterprise access to data"

Scope:	Data Strategy
Identifier/Title:	C1.1 - Facilitate access to sets of data at the enterprise level.
Description:	Refer to Deliverable 123.1.26 Enrollment Business Objectives and High-Level Requirements.

3.5.12 Business Objective C2.1 – "Enterprise policies and standards"

Scope:	Enrollment and Access Management
Identifier/Title:	C2.1 - Create enterprise policy and standards for enrollment and access management.
Description:	Refer to Deliverable 123.1.26 Enrollment Business Objectives and High-Level Requirements.

3.5.13 Business Objective C2.2 – "Security of FSA systems"

Scope:	Access Management	
Identifier/Title:	C2.2 - Maintain security of FSA systems.	
Description:	Previous FSA Security and Privacy Policy efforts outlined the FSA security fundamentals as individual accountability, least privilege, separation of duties and functions, principle of proportionality, and security and privacy by design. An access management system needs to be technically secure and support proper security procedures.	
High-Level Requirements:	C2.2.1	Provide secure infrastructure for access management.
	C2.2.2	Provide controls to mitigate risks associated with consolidated User IDs.
	C2.2.3	Provide centralized oversight of system security to identify potential security breaches.
	C2.2.4	Enforce individual accountability across FSA systems.
	C2.2.5	Establish enterprise-wide policy, participation agreements, and audits to limit a single User ID to a single user.
Additional Information	C2.2.2 – Increased convenience of a single User ID and single password also increases risks and any adverse consequences if this single User ID is compromised. C2.2.3 - As discussed in Business Objective B2.1, centralized enterprise-wide oversight will assist in the identification of potential security policy violations. C2.2.5 – A single User ID must not be shared across users. Multiple users sharing a single User ID violates the fundamental security principle of individual accountability.	

3.5.14 Business Objective C2.3 – "Match access privileges to job functions"

Scope:	Access Management	
Identifier/Title:	C2.3 - Provide users with access to FSA systems appropriate for their job function.	
Description:	A fundamental of FSA Security and Privacy Policy is least privilege – each individual is authorized access to only those FSA information assets required to perform his or her job. The definition of flexible role based users will help Access Management support this policy.	
High-Level Requirements:	C2.3.1	Provide role-based access to FSA systems.
	C2.3.2	Create flexible roles to allow for changes and additions independent of lifecycle phase.
	C2.3.3	Support exceptions to standard access roles.
	C2.3.4	Integrate Trading Partner access with Dept of Education Staff access processes.
	C2.3.5	Provide the ability to control access at different levels of granularity.
	C2.3.6	Support ability to designate the recipient of a requested file.
Additional Information	C2.3.1 - Create enterprise access roles based on job function. An enterprise role would define access across FSA systems based on the needs of the typical user. C2.3.2 & C2.3.3 – Job functions are not always easily characterized. The defined roles must remain flexible to support exceptions to the standard access role. (E.g. adding access privileges to a typical role or excluding certain privileges from a typical role.) C2.3.5 – Access should be controlled at different levels (e.g. system, window, field, data, etc.) C2.3.6 – This requirement refers specifically to the ability for a user to designate where a return file would be submitted (e.g. SAIG user). This requirement highlights the necessary interactions between the access management layer and individual system requirements. Access management identifies a user to a system but the system would need to allow the user choice of recipient locations.	

3.5.15 Business Objective C3.1 – "Effective training and customer support"

Scope:	Enrollment and Access Management
Identifier/Title:	C3.1 - Provide effective training and customer support across FSA systems.
Description:	Refer to Deliverable 123.1.26 Enrollment Business Objectives and High-Level Requirements.

3.5.16 Business Objective C3.1 – "Adopt policies to improve processes"

Scope:	Enrollment and Access Management
Identifier/Title:	C3.2 Adopt enrollment and access management policies that improve business processes.
Description:	Refer to Deliverable 123.1.26 Enrollment Business Objectives and High-Level Requirements.

3.6 Business Integration Group Vision Framework Cross Reference

	Enrollment and Access Management Business Objectives															
FSA BIG Vision Framework Objectives	A1.1 Enterprise process focus	A2.1 Manage across systems	A2.2 Self-service capabilities	A2.3 Balance access and security	A2.4 Flexibility for future requirements	A2.5 User customization	A3.1 Streamline enrollment and registration	B1.1 Uniform process for access decisions	B2.1 Audit user access	B3.1 Meet regulatory requirements	C1.1 Facilitate enterprise access to data	C2.1 Enterprise policies and standards	C2.2 Security of FSA systems	C2.3 Match access to job functions	C3.1 Effective training and support	C3.2 Adopt policies to improve processes
Easy customer access to required information throughout the delivery cycle	✓	✓	✓			✓	✓								✓	
Self-service capabilities			✓											✓		
Automated business processes		✓		✓			✓									
System-independent, integrated services to customers across the lifecycle		✓					✓							✓		
Standardized business processes	✓						✓								✓	✓
Easy and timely access to required oversight information								✓	✓						✓	
Efficient, automated oversight capabilities									✓							
Effective and balanced oversight									✓	✓						
Streamlined processes for routine oversight functions									✓							
Timely identification of risk-based non-compliance										✓						
Ability to proactively inform regulatory and statutory changes					✓					✓						
Actionable data to drive decision making											✓					
Deployment of technology solutions to meet program objectives		✓		✓	✓				✓			✓				✓
Clearly defined ownership and management of data														✓		
Consistent and accurate data across the enterprise											✓		✓	✓		
Maintain appropriately secured information				✓									✓	✓		
Flexible standards, technologies, services		✓			✓											✓
Tailored and relevant business services for all customer lifecycle activities							✓								✓	✓
Actionable information to inform business processes							✓								✓	
Effectively & efficiently manage organizational financial well-being		✓		✓												
Right skilled/trained workforce aligned with business processes															✓	
Maximize effectiveness of program based goals		✓														✓

Figure 3.3 - Cross reference of Enrollment and Access Management Objectives with related Business Integration Group (BIG) Vision Framework Objectives.

4 Conclusions and Next Steps

The Data Strategy Enrollment and Access Management task order started the process of reviewing and analyzing FSA's current processes for enrolling Trading Partners and for managing their access to FSA systems. The identification and documentation of FSA's Enrollment and Access Management Business Objectives and High-Level Requirements will be invaluable in the next phases of this effort.

This first phase of the Enrollment and Access Management task order produced the following guiding principles that will drive the high-level design:

- **Trading Partner Perception of FSA** - FSA enrollment and access management processes are a critical entry point for Trading Partners who wish to use FSA services. As initial point of contact, enrollment and access management processes greatly affect Trading Partner perceptions about the utility, usability, and customer service provided by FSA.
- **Phased Approach** - The 16 business objectives and 70 high-level requirements provide a broad perspective on required and desirable features of how FSA should interact with Trading Partners during the enrollment phase and during access management stages. They represent the most comprehensive set of views across FSA systems captured to date to describe how these processes should work. These objectives and requirements will provide an effective starting point for the analysis of solution options and development of high-level designs.
- **Access and Security** - FSA wishes to create more efficient and easier-to-use processes, but not at the expense of controls to protect FSA resources. Beyond regulatory compliance requirements, it makes good business sense for FSA to preserve the confidentiality and integrity of FSA data, and to safeguard the availability of its systems. There is a close relationship between methods for managing access to FSA systems and the enterprise security and privacy policies FSA wishes to enforce. FSA business objectives and the vision for the FSA security and privacy architecture will need to be coordinated and balanced to maximize the ability of FSA to achieve its business goals and still meet security objectives.
- **Enterprise Complexity** - Current FSA systems employ a variety of processes to accomplish similar enrollment and access management goals. The Participation Management system provides central services for several systems, but many standalone processes have been developed to satisfy the needs of individual systems. The FSA Enrollment and Access Management vision must accommodate the complexity and specific requirements of Participation Management and the isolated systems while aiming toward consolidation and simplification of processes when possible.
- **Solution Flexibility** - FSA systems will not remain static. A number of system reengineering and consolidation efforts are already underway. New and developing technologies will become integrated into the FSA environment. A variety of other examples were also brought up during workshops and interviews that illustrate the

need to include flexibility requirements in the enrollment and access management vision.

- **Technology** - Many of the FSA high-level requirements for enrollment and access management involved new functions that may require additional technologies or technical solutions. Examples identified during working sessions include enterprise access management across multiple systems, single sign-on functions, automation of enrollment and access management, and user self-service capabilities. Before they are incorporated into the FSA vision or high-level designs, technical components will need to be carefully evaluated to make sure they represent an appropriate balance between functionality and cost.
- **Effective Communication Processes** - Enrollment and Access Management systems are important as entry points and ongoing contact points for FSA Trading Partners. Interactions with Trading Partners can be effective communications channels that FSA can leverage for a variety of purposes. As several participants pointed out, FSA should have well-defined and effective communications processes that provide users with consistent messages and efficient user support for enrollment and access management.
- **Other FSA Initiatives** - Enrollment and Access Management must be coordinated with several other projects across the enterprise. Integration of this effort with RID and other Data Strategy projects will provide a foundation for streamlining Trading Partner enrollment and user access management across the enterprise. This effort must also be coordinated with the FSA Security Architecture development work, Integrated Partner Management responsibilities, Case Management Oversight efforts, and the PIN Site Reengineering project.
- **Benefits** - Enrollment and Access Management will create a vision for an enterprise approach to enrolling and managing access for Trading Partners. Consolidated processes and tools will improve FSA control of critical enrollment and access management functions, increasing the efficiency of these processes and decreasing administrative costs. Most importantly, an enterprise approach will insulate Trading Partners from the complexities of the internal FSA enrollment and access management processes and improve the effectiveness of FSA service delivery.

Next steps for the Enrollment and Access Management Team will include the following tasks:

- **Validate Business Objectives and High-Level Requirements** - Enrollment and Access Management must continue validating these Business Objectives and High-Level Requirements as a proposed vision for Enrollment and Access Management is created.
- **Determine Priority of Business Objectives** - These Business Objectives and High Level Requirements were documented without trying to determine relative priorities or deployment impacts. The Enrollment and Access Management team will facilitate a process to help FSA prioritize these requirements during the early stages of high-level design.
- **Develop High-Level Designs** - The Enrollment and Access Management Team will facilitate working sessions to develop and document high-level designs for a recommended solution. Additional meetings with individual systems and groups of

systems will be conducted to assess the effectiveness of proposed high-level designs and to engage stakeholders in the development of appropriate business cases.

- **Communicate the Vision** - Enrollment and Access Management must work to socialize and communicate the eventual Enrollment and Access Management Vision throughout the FSA CIO organization and FSA business units.

Appendix A: Security Definitions of Access Management and Identity Management

During interviews, meetings, and working sessions to identify business objectives, the term "access management" was used in a broad sense to include all topics related to registering and gaining access to FSA systems and applications. This usage considered "access" to include user authentication, access control, administration of system user access accounts, development of access authorization policies, and the processes and forms used to approve a user request for access. The Enrollment and Access Management Team have used this broad definition of access management in this document, with appropriate qualification as necessary to maintain clarity.

In the field of information security, a more common definition of "access management" reserves this term for the authentication of users and direct control or restriction of user access to information resources. In other words, "access" in this sense refers to "front-end" security processes that directly meditate real-time user interactions with systems and applications, such as login and control of a user session. "Single Sign-on" functions would also fall under the definition of access management. This more restrictive definition of access management was used in the recently completed Security and Privacy Architecture Framework project. The boxes that fall within the dashed lines in Figure A1 illustrate the functions and processes that fit this definition.

In contrast, the concept of "Identity Management" is gaining wide acceptance as the term for "back-end" processes and tools, such as those that control authorization steps and processes for granting and configuring user access. Used in this sense, "identity management" covers processes and technologies for administration of access, including registration of users, security approval workflow tools, automation of security administration processes, password synchronization, delegation of administration, auditing access privileges, and management of data repositories for user identity information. The dotted-line box in Figure A1 depicts processes and functions usually considered to fall within "Identity Management".

Access management and identity management must be closely integrated to effectively enforce an organization's information access and security policies. Technology implementations of these security systems often share functions and components, such as the data repositories for storing user attributes and identity information. Some security vendor products combine functional capabilities from these two categories. In fact, a long-term goal in the information security world is to fully integrate access and identity management systems. This integration of access and identity management is currently feasible only in an environment that contains web applications and components. However, the distinction between management of access and identity remains important in an enterprise environment that extends beyond web applications. The technologies available to implement access management functions and identity management are quite different for legacy and mainframe systems.

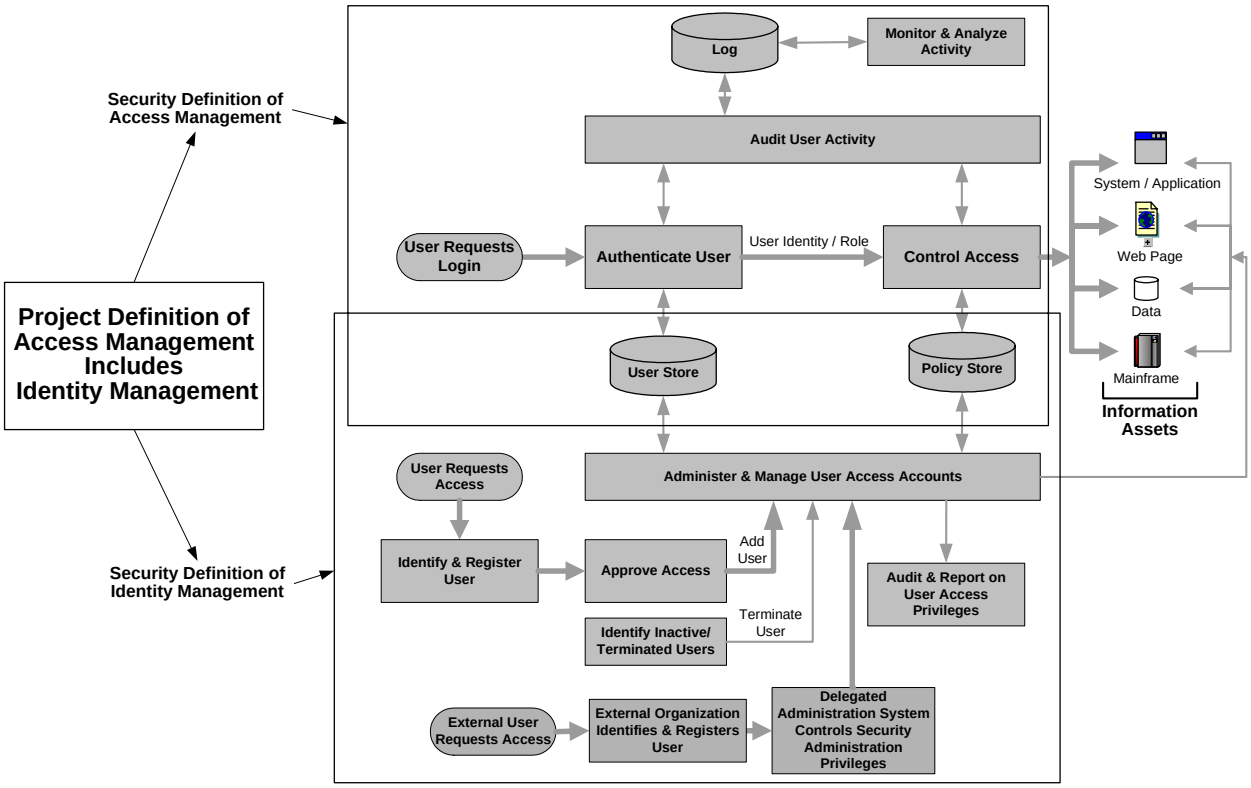


Figure A1 - Security Functions and Processes That Comprise Access Management and Identity Management

Appendix B: Business Objective Meeting Summaries

Refer to the Appendix_B_BusinessObjectiveSummaries.doc file or the printed copy of Deliverable 123.1.26.

Appendix C: Questionnaires

Refer to the Appendix_C_Questionnaires.doc file or the printed copy of Deliverable 123.1.26.

Appendix D: Business Integration Group Vision Framework

Refer to the Appendix_D_DRAFT BIG Integration Vision Framework v5.xls file or the printed copy of Deliverable 123.1.26.

Appendix E: Enrollment and Access Management Business Objectives Vision Framework

Refer to the Appendix_E_EAM Business Obj Vision Framework v22.xls file or the printed copy of Deliverable 123.1.26.